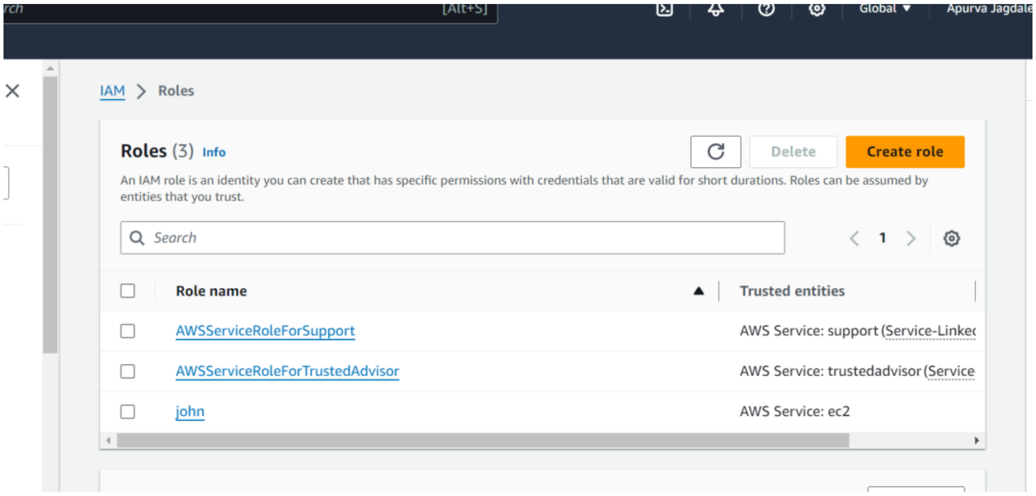
ROLES

TASK I : Create a role in IAM service

Step I : go to in IAM service then click on Roles then Click to create Role.

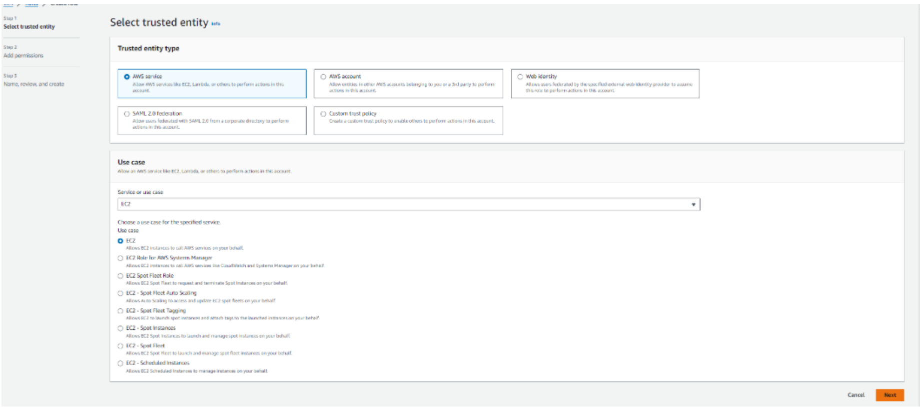


Roles (3) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linkec
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service
□	john	AWS Service: ec2

Step II : Select the AWS Service in Trusted Entity Type and also Select the Service or use case then choose the usercase for the Specified Service then click on Next.



Select trusted entity

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case: EC2 ▾

Choose a use case for the specified service.

Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

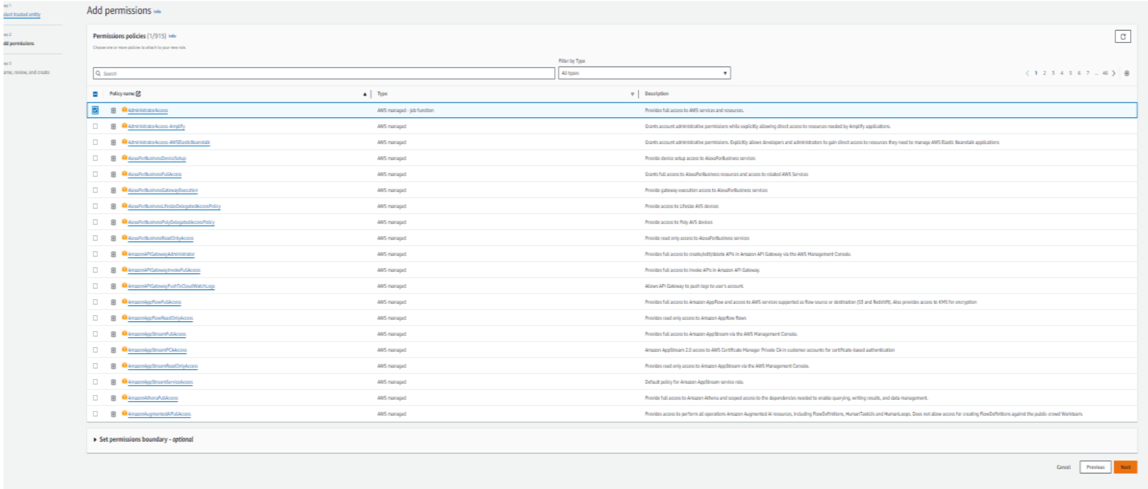
○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Step III : Add the Permission in Permissions Policies which you want to give and then on Next.



Add permissions

Permissions policies (1/915)

Choose one or more policies to attach to your new role.

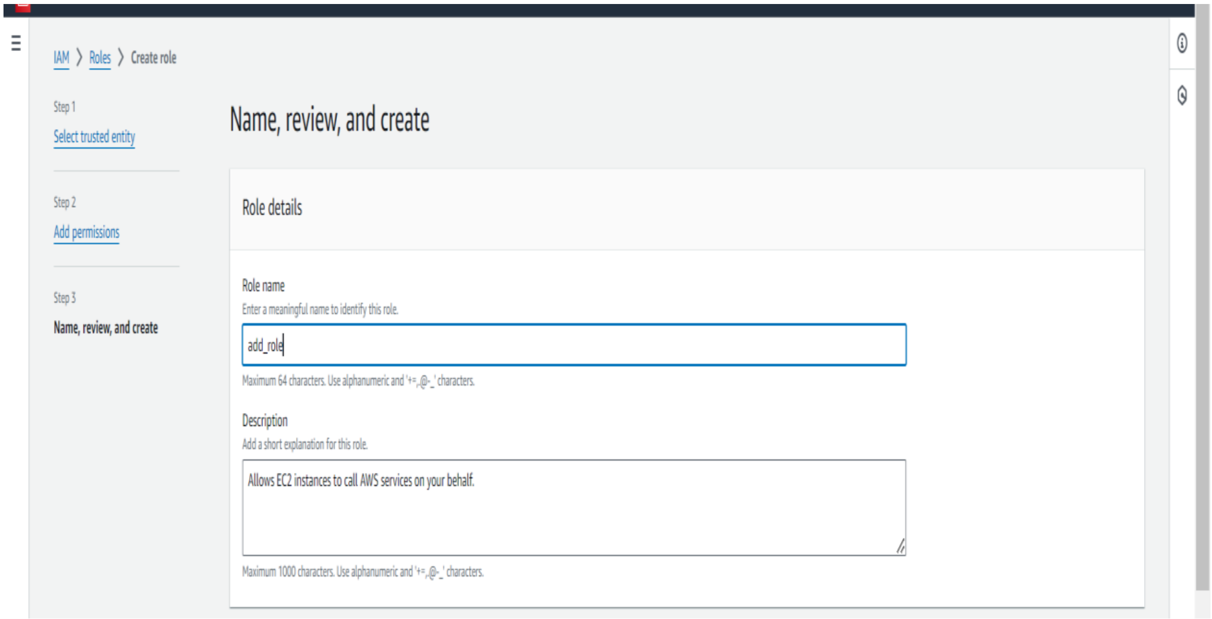
Search

Filter by Type: All types

	Policy name	Type	Description
☑	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.
□	AdministratorAccess-Amplify	AWS managed	Grants account administrative permissions while explicitly allowing direct access to resources needed by Amplify applications.
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permissions. Explicitly allows developers and administrators to gain direct access to resources they need to manage AWS Elastic Beanstalk applications
□	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to AlexaForBusiness services
□	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusiness resources and access to related AWS Services
□	AlexaForBusinessGatewayExecution	AWS managed	Provide gateway execution access to AlexaForBusiness services
□	AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	Provide access to Lifesize AVS devices
□	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	Provide access to Poly AVS devices
□	AlexaForBusinessReadOnlyAccess	AWS managed	Provide read only access to AlexaForBusiness services
□	AmazonAPIGatewayAdministrator	AWS managed	Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
□	AmazonAPIGatewayInvokeFullAccess	AWS managed	Provides full access to invoke APIs in Amazon API Gateway.
□	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	Allows API Gateway to push logs to user's account.
□	AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlow and access to AWS services supported as flow source or destination (S3 and Redshift). Also provides access to KMS for encryption
□	AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon Appflow flows
□	AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStream via the AWS Management Console.
□	AmazonAppStreamPCAAccess	AWS managed	Amazon AppStream 2.0 access to AWS Certificate Manager Private CA in customer accounts for certificate-based authentication
□	AmazonAppStreamReadOnlyAccess	AWS managed	Provides read only access to Amazon AppStream via the AWS Management Console.
□	AmazonAppStreamServiceAccess	AWS managed	Default policy for Amazon AppStream service role.
□	AmazonAthenaFullAccess	AWS managed	Provide full access to Amazon Athena and scoped access to the dependencies needed to enable querying, writing results, and data management.
□	AmazonAugmentedAIFullAccess	AWS managed	Provides access to perform all operations Amazon Augmented AI resources, including FlowDefinitions, HumanTaskUis and HumanLoops. Does not allow access for creating FlowDefinitions against the public-crowd Workteam.

▸ Set permissions boundary - optional

Step IV :Give the Meaningful name to identify this role.



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

add_role

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

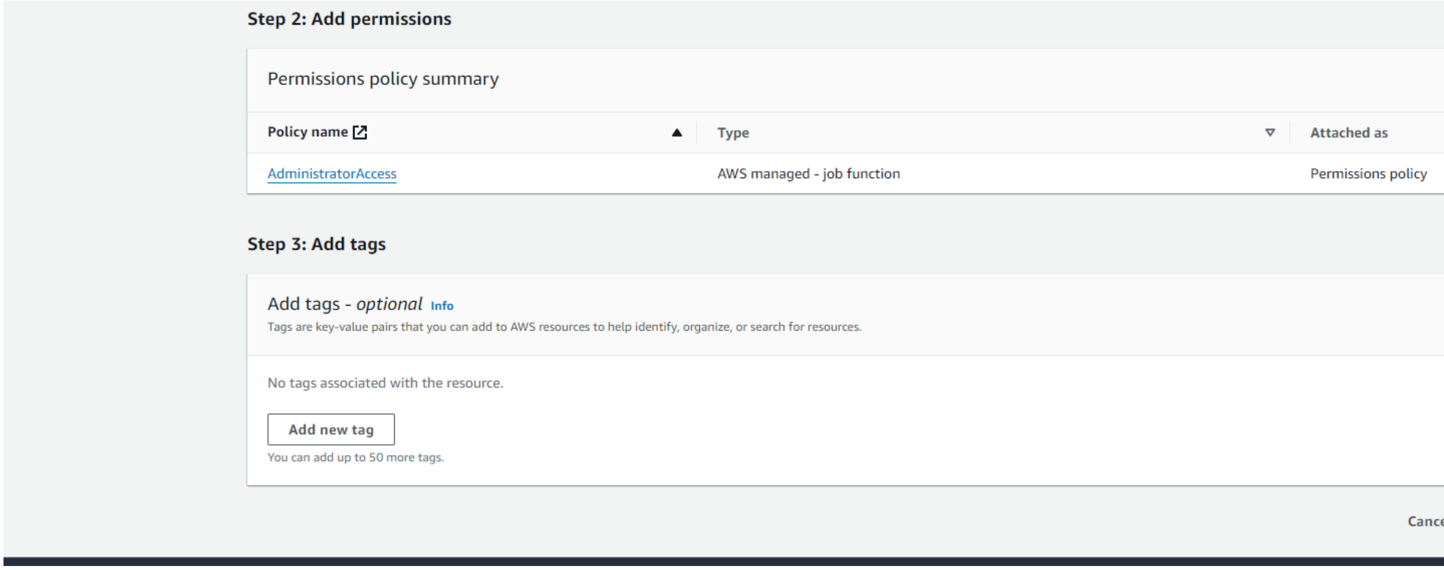
Description

Add a short explanation for this role.

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step V : Select the permission which you want to give any other then click on edit option then Select Permission and add it and then click on the create role tab



Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AdministratorAccess	AWS managed - job function	Permissions policy

Step 3: Add tags

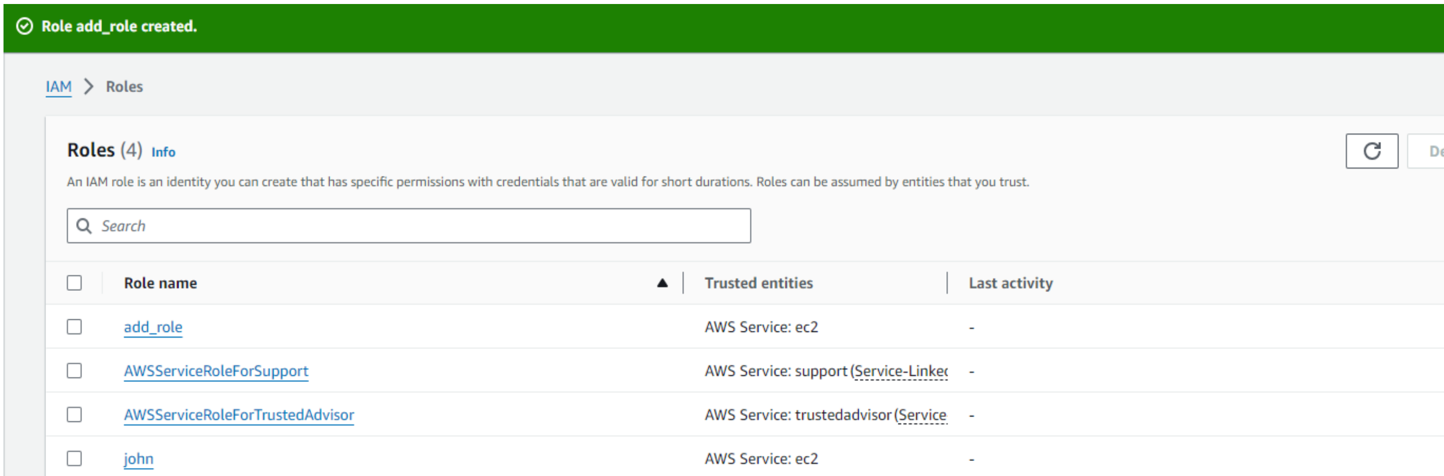
Add tags - *optional* Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

Step VI : Now,Role is Created here.



Role add_role created.

Roles (4) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

☐	Role name	Trusted entities	Last activity
☐	add_role	AWS Service: ec2	-
☐	AWSServiceRoleForSupport	AWS Service: support (Service-Linkec	-
☐	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
☐	john	AWS Service: ec2	-

TASK II : DOWNLOAD AND INSTALL AWSCLI PROPERLY AND THEN LOGIN USER ON CLI.

Step I :Download and Install AWS-CLI using above link for Windows.

https://awscli.amazonaws.com/AWSCLIV2.msi

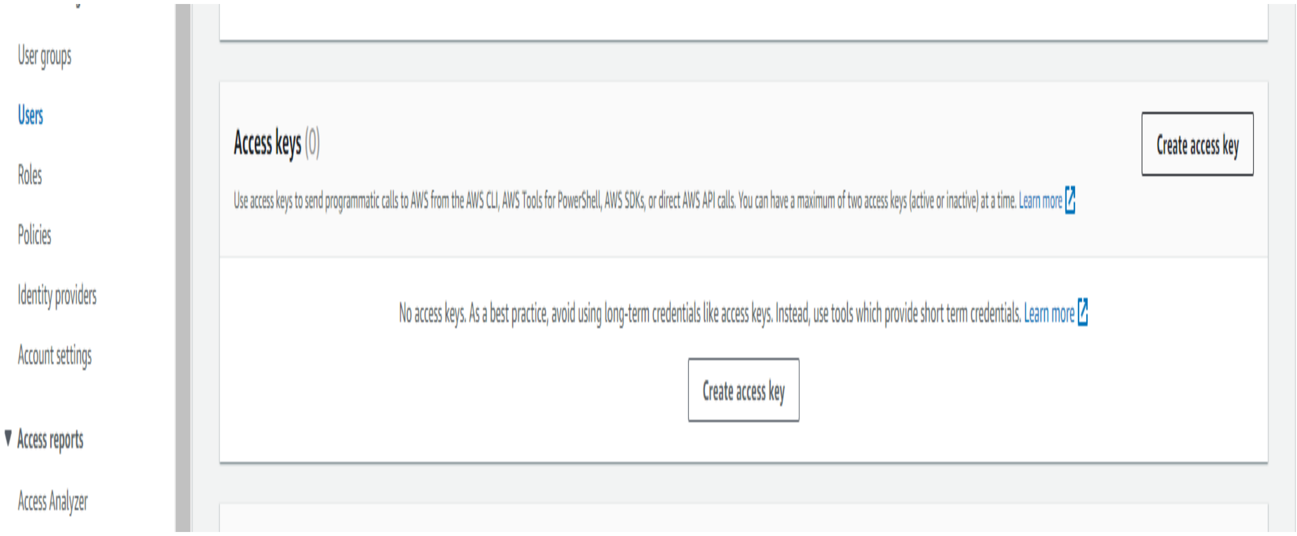
Step II : Open the as a Administrator Command Prompt and then execute the “aws – version” command to check the software is downloaded and Installed Properly.

Step III : If it is Installed properly it will show you AWS-CLI is an Executable Type.

Step IV : Then Execute the Command “aws configure” to configure the user.

Step V: It will Request access key from you .

Step VI : then return to your console and go to IAM service, Click on Users, Choose Create Access key

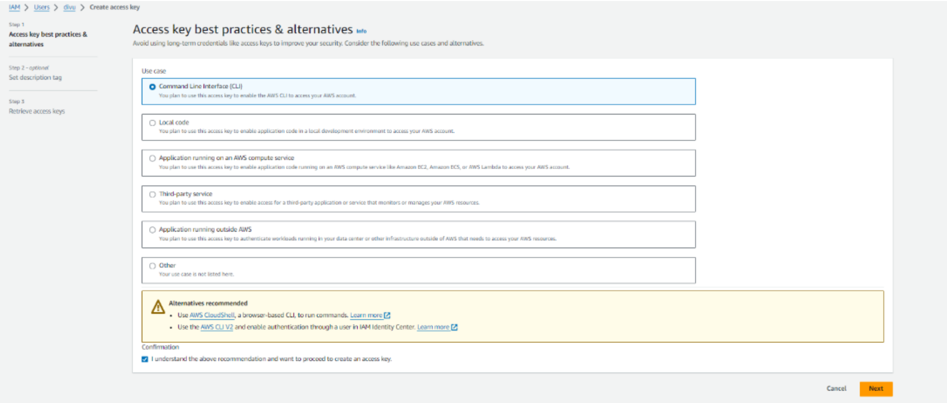


Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Step VII : In Use case select the Command Line Interface then also click on confirmation and then Next.


IAM > Users > divu > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Cancel
Next

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

● Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

○ Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

○ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

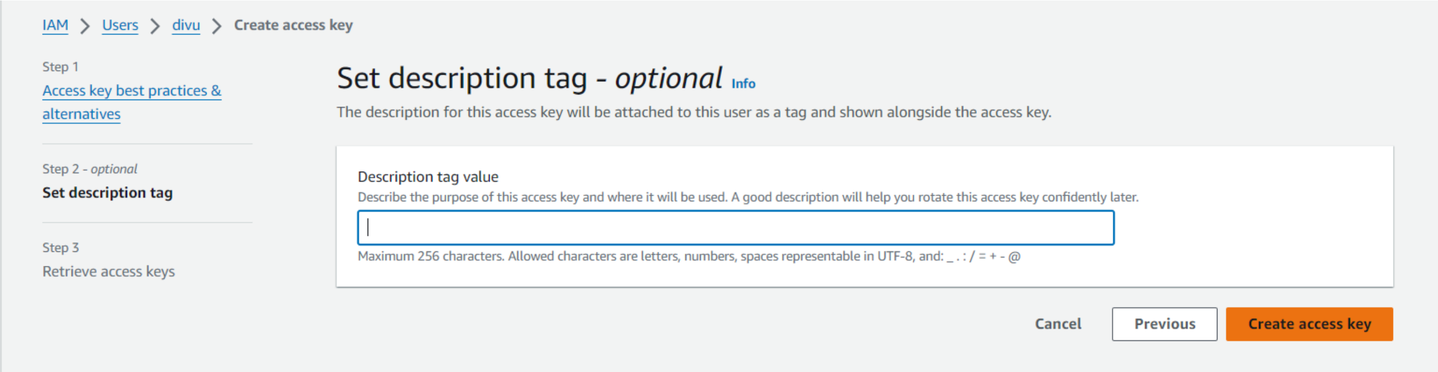
○ Other
Your use case is not listed here.

Alternatives recommended
- Use AWS CloudShell, a browser-based CLI, to run commands. Learn more
- Use the AWS CLI V2 and enable authentication through a user in IAM Identity Center. Learn more

Confirmation

☑ I understand the above recommendation and want to proceed to create an access key.

Step VIII : if you want to set Description tag then set it otherwise it’s Optional and at last click on create key tab.



Set description tag - *optional* Info

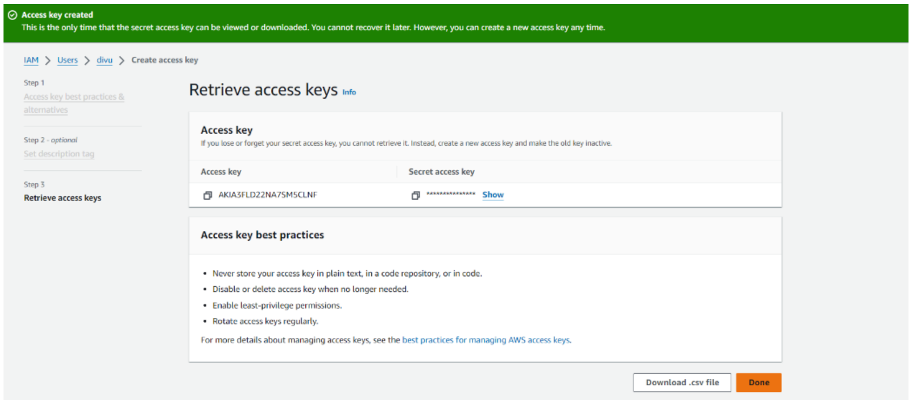
The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Step IX: And Here Access Key Created Successfully.



Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIA3FLD22NA7SM5CLNF	*************** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

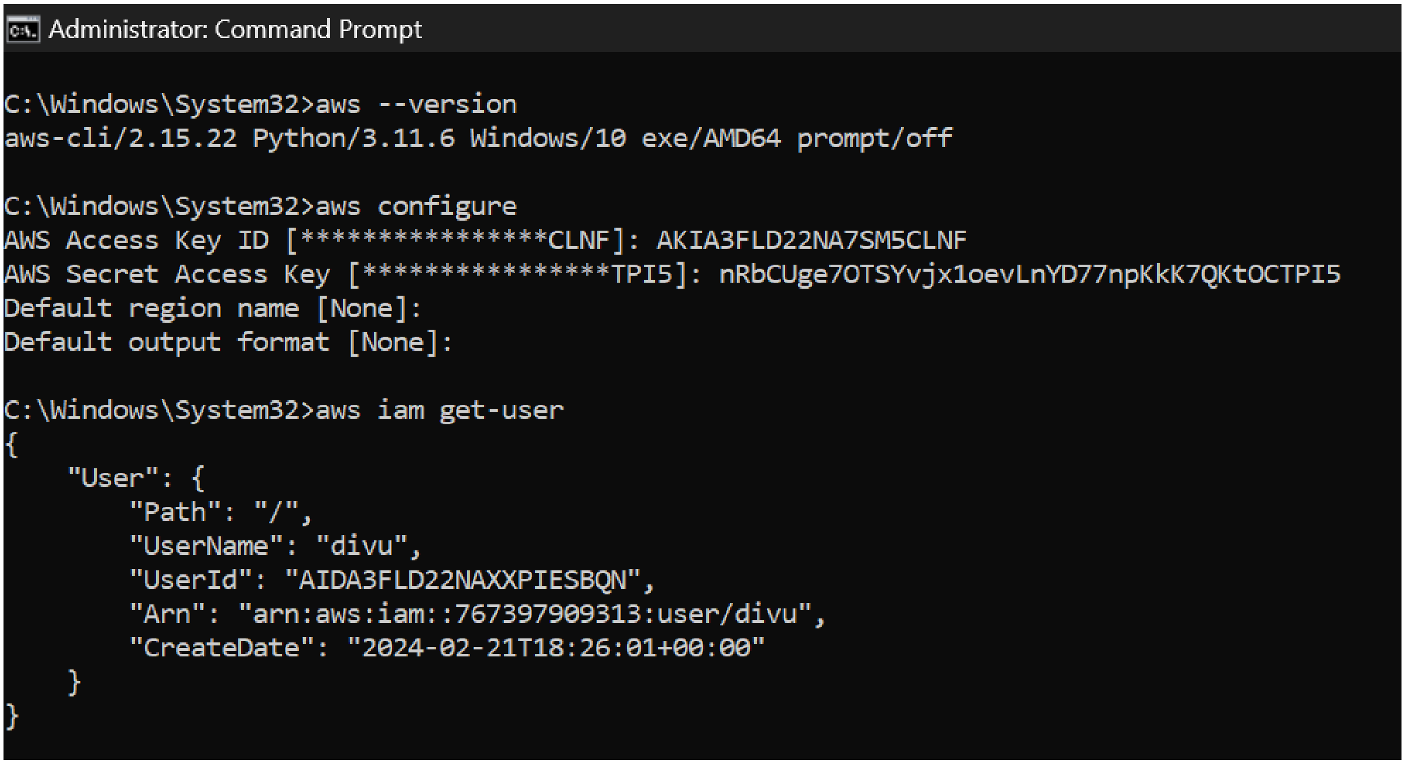
For more details about managing access keys, see the best practices for managing AWS access keys.

Step X : Copy the Access Key and paste it into the terminal where it says Access Key ID, and then copy the Secret access Key and paste it into the terminal.

Step XI : Specify the default region name and Default Output Format.

Step XII : Then Enter the Command “aws iam get-user” to view the details about the current login user in CLI.

Step XIII : The user is now logged in using CLI with administrator permissions.



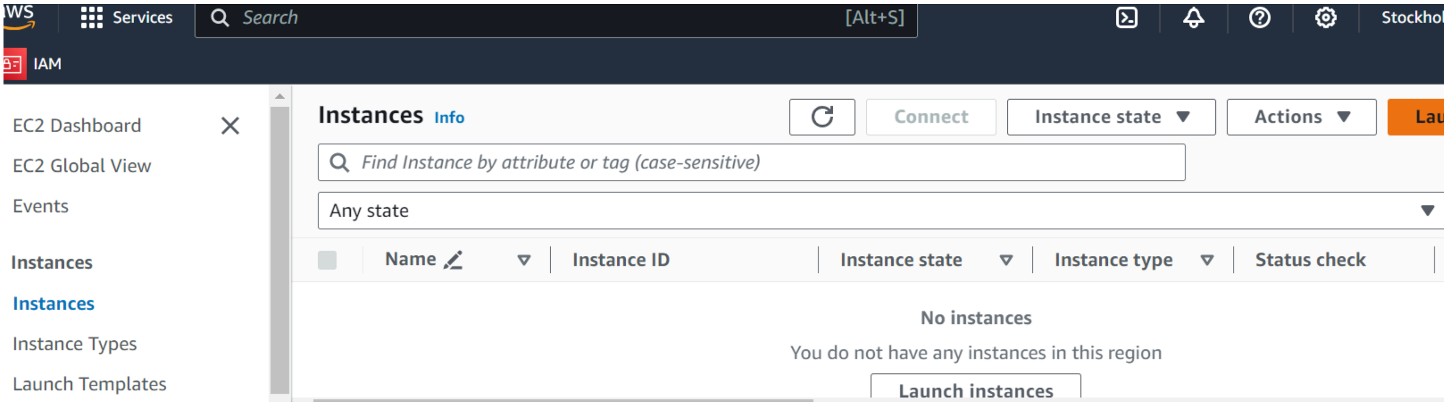
```
C:\Windows\System32>aws --version
aws-cli/2.15.22 Python/3.11.6 Windows/10 exe/AMD64 prompt/off

C:\Windows\System32>aws configure
AWS Access Key ID [****************CLNF]: AKIA3FLD22NA7SM5CLNF
AWS Secret Access Key [****************TPI5]: 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
Default region name [None]:
Default output format [None]:

C:\Windows\System32>aws iam get-user
{
    "User": {
        "Path": "/",
        "UserName": "divu",
        "UserId": "AIDA3FLD22NAXXPIESBQN",
        "Arn": "arn:aws:iam::767397909313:user/divu",
        "CreateDate": "2024-02-21T18:26:01+00:00"
    }
}
```

The Credential file is saved in C:\Users\lenovo\.aws\credentials

They can control login information. So, the Roles are used for same Purpose.

TASK III : How the user login without credentials using the EC2 instance ??

Step I : In Services search the EC2 click on it. In instance, click the Lauch Instance.

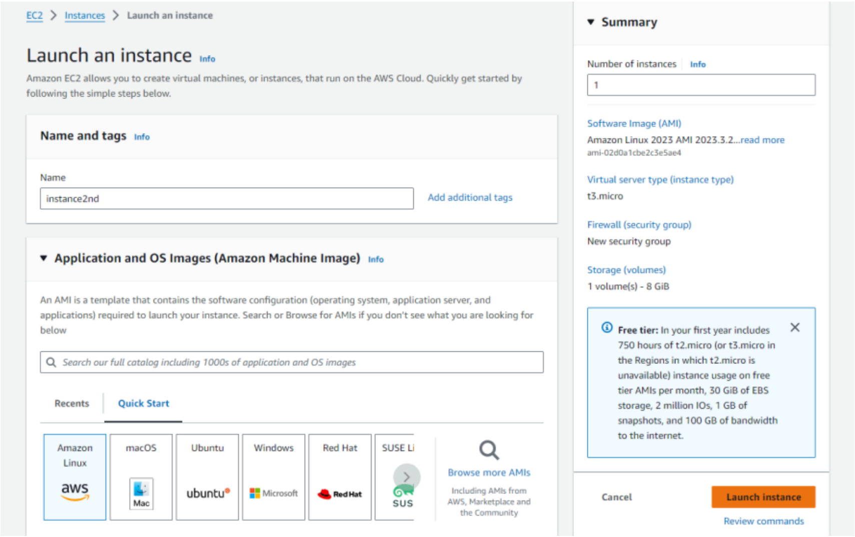


Name	Instance ID	Instance state	Instance type	Status check

No instances

You do not have any instances in this region

Step II : then give the name for instance and select Application and Os Images. Then launch Instance.



Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: instance2nd

Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Number of instances: 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-02d0a1cbe2c3e5ae4

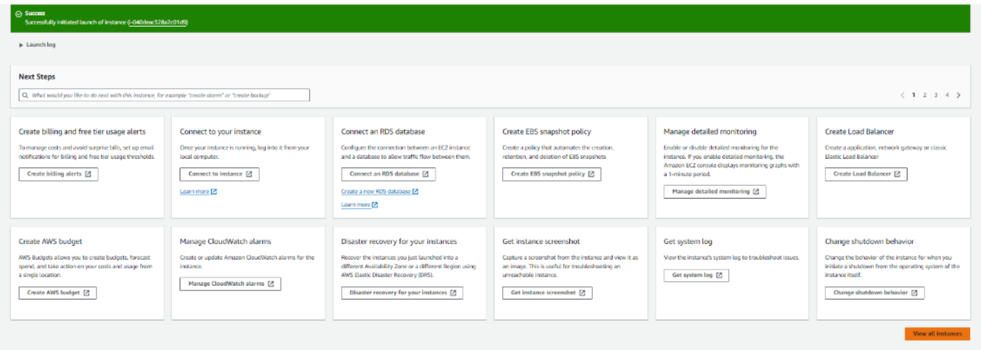
Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Step III : Click on View all Instances.



Success

Successfully initiated launch of instance (i-040deac328a2c01d9)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

Disaster recovery for your instances

Recover the instances you just launched into a different Availability Zone or a different Region using AWS Elastic Disaster Recovery (DRS).

Get instance screenshot

Capture a screenshot from the instance and view it as an image. This is useful for troubleshooting an unreachable instance.

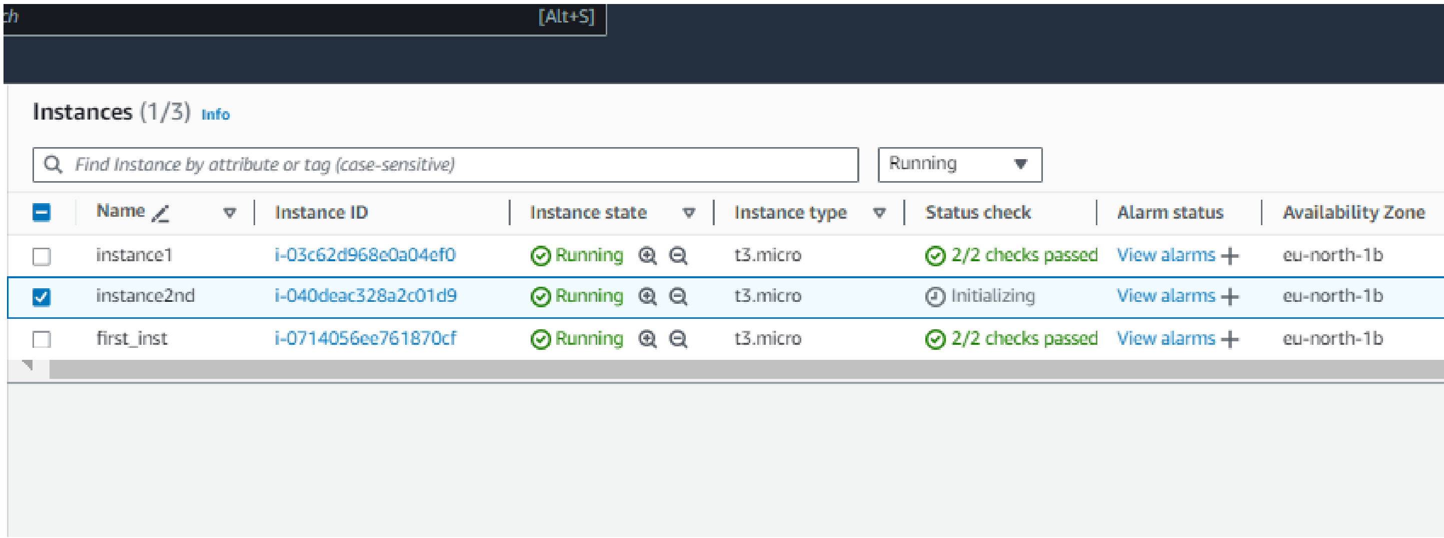
Get system log

View the instance's system log to troubleshoot issues.

Change shutdown behavior

Change the behavior of the instance for when you initiate a shutdown from the operating system of the instance itself.

Step IV : then Select the Instance, In Actions select Security and in Security Select Modify IAM role and select the role and Update it.

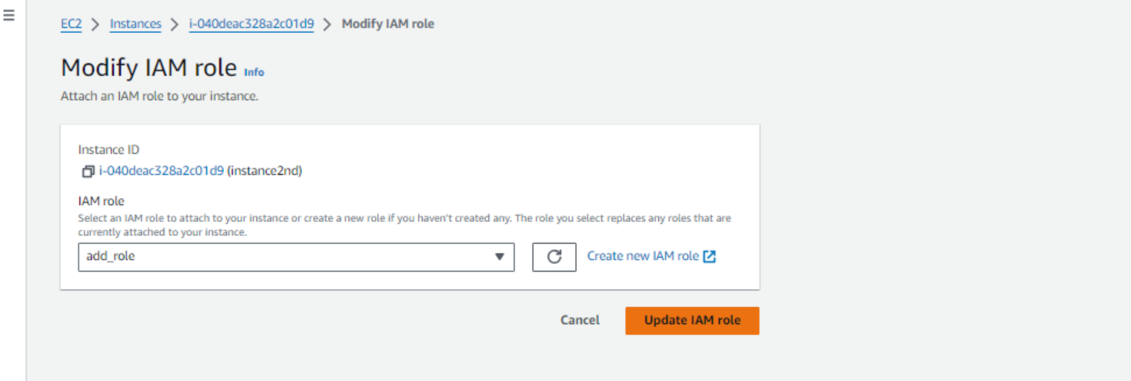


Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive)

Running

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☐	instance1	i-03c62d968e0a04ef0	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b
☑	instance2nd	i-040deac328a2c01d9	Running	t3.micro	Initializing	View alarms +	eu-north-1b
☐	first_inst	i-0714056ee761870cf	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b



EC2 > Instances > i-040deac328a2c01d9 > Modify IAM role

Modify IAM role Info

Attach an IAM role to your instance.

Instance ID

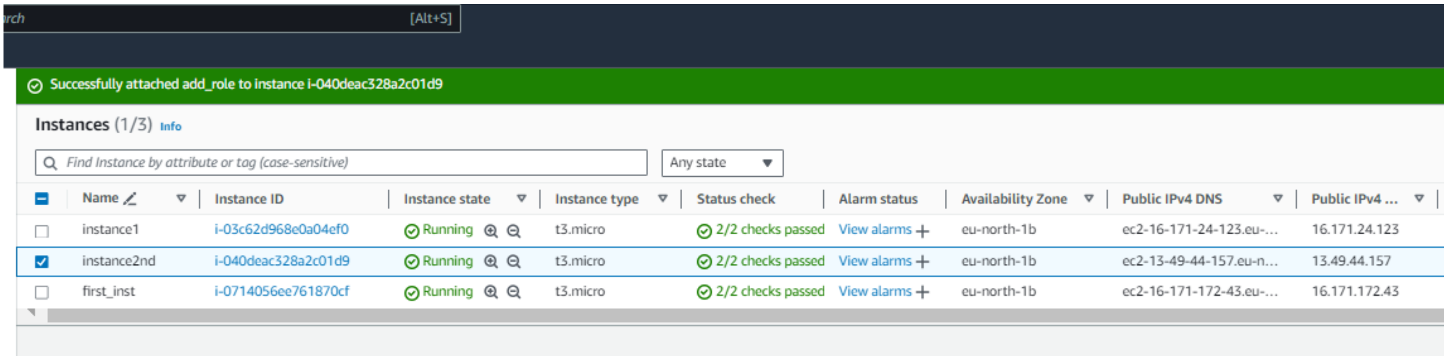
i-040deac328a2c01d9 (instance2nd)

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

add_role

Step V : Click to Connect Button and Select the Connection Type and then Connect it.



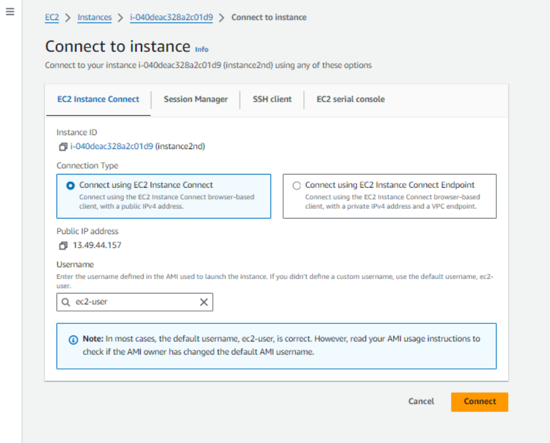
rch [Alt+S]

Successfully attached add_role to instance i-040deac328a2c01d9

Instances (1/3) Info

Find Instance by attribute or tag (case-sensitive) | Any state

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☐	instance1	i-03c62d968e0a04ef0	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b	ec2-16-171-24-123.eu-...	16.171.24.123
☑	instance2nd	i-040deac328a2c01d9	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b	ec2-13-49-44-157.eu-n...	13.49.44.157
☐	first_inst	i-0714056ee761870cf	Running	t3.micro	2/2 checks passed	View alarms +	eu-north-1b	ec2-16-171-172-43.eu-...	16.171.172.43



EC2 > Instances > i-040deac328a2c01d9 > Connect to instance

Connect to instance Info

Connect to your instance i-040deac328a2c01d9 (instance2nd) using any of these options

Instance ID
i-040deac328a2c01d9 (instance2nd)

Connection Type

● Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

○ Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

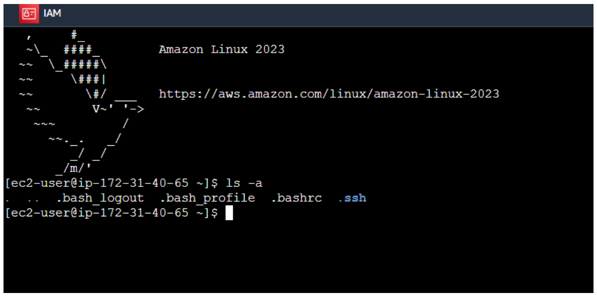
Public IP address
13.49.44.157

Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.

ec2-user

Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Step VI : After Establishing connection it is Connected. now, there won’t be file with Credentials to see this, execute the ls -a command here . we can give all administrators command because we give the permission here to role is Administrator full access.



```
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-40-65 ~]$ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .ssh
[ec2-user@ip-172-31-40-65 ~]$ 
```